Clase 6 — 11.12.25

#ciscopackettracer #network

👨‍🏫 **Profesor:** Carlos Quintana
📘 **Unidad:** Ciberseguridad
🗓️ **Fecha:** 11/12/2025
🎯 **Tema:** Repaso Autoevaluación Diciembre 2025

🔐 REPASO AUTOEVALUACIÓN

1️⃣ ¿Qué se entiende por *Sniffer*?

🔹 Definición base

Un **sniffer** es una herramienta o técnica que permite **capturar y analizar el tráfico de red** que circula por una interfaz de red.

Dicho de forma simple:

> Un sniffer “escucha” los paquetes que viajan por la red.

🔹 Qué hace realmente un sniffer (a nivel de red)

Un sniffer puede ver:

- Direcciones IP de origen y destino
- Puertos utilizados
- Protocolos (HTTP, FTP, DNS, etc.)
- Contenido del paquete **si no está cifrado**

📌 Ejemplo:

- Usuario accede a una web sin HTTPS
- El sniffer puede ver:
  - Usuario
  - Contraseña
  - Contenido de la comunicación

🔹 Relación directa con lo visto en clase (Firewall y VPN)

En las clases anteriores habéis visto que:

- El **firewall ASA**:
  - Filtra tráfico
  - Decide qué entra y qué no
- La **VPN**:
  - Cifra el tráfico

👉 El sniffer **no rompe nada**, simplemente **aprovecha**:

- Tráfico sin cifrar
- Redes mal protegidas

Por eso:

- HTTPS
- SSH
- VPN
  son **defensas directas contra sniffing**.

🔹 Uso legítimo vs uso malicioso

✔ Uso legítimo:

- Diagnóstico de red
- Análisis de problemas
- Auditorías de seguridad

❌ Uso malicioso:

- Robo de credenciales
- Espionaje
- Preparación de ataques posteriores

📌 En ciberseguridad:

> El sniffer es una herramienta.
> El problema es **quién y para qué la usa**.

🔹 Respuesta tipo examen

Un sniffer es una herramienta que permite capturar y analizar el tráfico de red entre equipos y servidores, pudiendo visualizar información sensible si el tráfico no está cifrado.

2️⃣ ¿Qué se entiende por *Phishing*?

🔹 Definición base

El **phishing** es un ataque de **ingeniería social** en el que un atacante **suplanta la identidad** de una persona o empresa legítima para **engañar al usuario** y robar información sensible.

🔹 Qué información se roba habitualmente

- Contraseñas
- Datos bancarios
- DNI
- Correos corporativos
- Credenciales de empresa

📌 El ataque **no va contra el sistema**, va contra la persona.

🔹 Cómo funciona un ataque de phishing

1. El atacante envía:
   - Correo
   - SMS
   - Mensaje
2. Se hace pasar por:
   - Banco
   - Empresa
   - Administrador
3. El usuario:
   - Confía
   - Introduce sus datos
4. El atacante:
   - Los roba
   - Accede a sistemas reales

🔹 Relación con AAA (clases anteriores)

Habéis visto **AAA**:

- Autenticación
- Autorización
- Contabilización

El phishing **rompe la autenticación**, porque:

- El atacante obtiene las credenciales legítimas
- El sistema cree que el usuario es válido

👉 Por eso:

- AAA es necesario
- Pero **no suficiente** si el usuario cae en phishing

🔹 Por qué el firewall no protege del phishing

El firewall:

- Filtra tráfico
- No distingue si el usuario **decide** entregar su contraseña

📌 Conclusión clave:

> El phishing bypassa la seguridad técnica explotando el factor humano.

🔹 Respuesta tipo examen

El phishing es un ataque en el que un delincuente se hace pasar por una persona o empresa de confianza para engañar al usuario y robar información sensible como contraseñas o datos bancarios.

3️⃣ ¿Qué se entiende por *Spoofing*?

🔹 Definición base

El **spoofing** es una técnica de **suplantación de identidad** en la que un atacante **falsea su identidad** para hacerse pasar por otro dispositivo, usuario o servicio.

🔹 Tipos comunes de spoofing

- **IP Spoofing** → falsear IP
- **MAC Spoofing** → falsear MAC
- **DNS Spoofing** → falsear respuestas DNS
- **ARP Spoofing** → engañar a la red local

🔹 Qué consigue un atacante con spoofing

- Engañar a otros sistemas
- Redirigir tráfico
- Interceptar comunicaciones
- Preparar ataques mayores

📌 Spoofing suele ser **fase previa** a:

- Sniffing
- Man-in-the-Middle
- Robo de credenciales

🔹 Relación con firewall y niveles de seguridad

En el laboratorio del ASA:

- El firewall:
  - No confía solo en IP
  - Usa niveles de seguridad
  - Aplica reglas estrictas

👉 Esto dificulta el spoofing porque:

- No basta con “parecer” interno
- El tráfico sigue pasando por el firewall

🔹 Respuesta tipo examen

El spoofing es una técnica de suplantación de identidad en la que un atacante se hace pasar por otro usuario o dispositivo para engañar a los sistemas de la red.

4️⃣ ¿Qué se entiende por *Denegación de Servicio* (DoS)?

🔹 Definición base

Un ataque de **Denegación de Servicio (DoS)** consiste en **saturar un sistema, red o servicio** con tráfico o peticiones inútiles para impedir que los usuarios legítimos puedan utilizarlo.

🔹 Qué provoca un DoS

- Caída del servicio
- Lentitud extrema
- Bloqueo del sistema
- Pérdida de disponibilidad

📌 El objetivo **no es robar**, sino **interrumpir**.

🔹 Cómo funciona un DoS (concepto)

- El atacante envía:
  - Miles o millones de peticiones
- El servidor:
  - Consume recursos
  - No puede atender a usuarios reales

🔹 Relación directa con el firewall ASA

En clase habéis visto que:

- El firewall:
  - Filtra tráfico
  - Bloquea patrones
  - Limita accesos

👉 El firewall es **la primera defensa contra DoS**, porque:

- Puede bloquear tráfico anómalo
- Puede limitar conexiones
- Puede proteger servicios internos

🔹 Diferencia con DDoS (nota importante)

- **DoS** → un solo atacante
- **DDoS** → muchos equipos (botnet)

🔹 Respuesta tipo examen

Una denegación de servicio es un ataque en el que se satura un equipo o servidor con tráfico inútil para impedir que los usuarios legítimos puedan utilizar los servicios normales.

5️⃣ Crear copias de seguridad es seguridad… PASIVA

🔹 Definición base

Las **copias de seguridad (backups)** forman parte de la **seguridad pasiva**, porque:

- ❌ No evitan ataques
- ❌ No bloquean accesos
- ✔ Actúan **después** de que ocurra un problema

📌 Sirven para **recuperar**, no para **proteger activamente**.

🔹 Qué protege realmente un backup

Un backup protege frente a:

- Fallos de hardware
- Errores humanos
- Borrados accidentales
- Ransomware (si es recuperable)

👉 **No protege** frente a:

- Phishing
- Sniffing
- Spoofing
- DoS

🔹 Relación con lo visto en firewall y ASA

En las prácticas del ASA:

- El firewall es **seguridad activa**
- Filtra tráfico en tiempo real

El backup, en cambio:

- No participa en la red
- No analiza paquetes
- No decide accesos

📌 Es la última red de seguridad cuando todo lo demás falla.

🔹 Analogía clara

- Firewall → **puerta blindada**
- Antivirus → **alarma**

- Backup → **copia de las llaves y documentos en una caja fuerte**

🔹 Respuesta tipo examen

Las copias de seguridad son seguridad pasiva, ya que no evitan ataques, pero permiten recuperar la información tras un fallo o incidente.

6️⃣ Un antivirus sería seguridad… ACTIVA

🔹 Definición base

Un **antivirus** es seguridad **activa** porque:

- Analiza el sistema constantemente
- Detecta comportamientos maliciosos
- Bloquea amenazas en tiempo real

📌 No espera a que el daño esté hecho.

🔹 Qué hace un antivirus a nivel práctico

- Escanea archivos
- Analiza procesos
- Detecta firmas y comportamientos
- Aísla o elimina malware

👉 Actúa **mientras el sistema está funcionando**.

🔹 Relación directa con lo visto en clase

En clase se explicó:

> Si el malware pasa el firewall, entra en juego el antivirus.

Esto define claramente:

- Firewall → primera línea
- Antivirus → segunda línea

📌 Seguridad por capas (defense in depth).

🔹 Por qué es seguridad activa

Porque:

- Reacciona automáticamente
- No depende del usuario
- Toma decisiones de bloqueo

🔹 Respuesta tipo examen

Un antivirus es seguridad activa porque detecta y bloquea amenazas en tiempo real cuando el sistema está en funcionamiento.

7️⃣ Un cortafuegos (firewall) sería seguridad… ACTIVA

🔹 Definición base

Un **firewall** es seguridad activa porque:

- Filtra tráfico de red
- Decide qué entra y qué sale
- Aplica reglas constantemente

📌 Está siempre “trabajando”.

🔹 Relación directa con el ASA visto en clase

El **Cisco ASA**:

- Filtra por:
  - IP
  - Puerto
  - Protocolo
  - Usuario (AAA)
- Aplica:
  - Niveles de seguridad
  - Deny by default

👉 Todo esto ocurre **en tiempo real**.

🔹 Qué pasaría sin firewall

- Accesos directos a PCs internos
- Ping desde Internet
- Escaneos
- Ataques directos

📌 El firewall es el **portero** de la red.

🔹 Respuesta tipo examen

Un cortafuegos es seguridad activa porque filtra y controla el tráfico de red en tiempo real, permitiendo o bloqueando comunicaciones según las reglas configuradas.

8️⃣ ¿Qué se entiende por AAA?

🔹 Definición base

AAA significa:

- **A**utenticación
- **A**utorización
- **A**uditoría (o Contabilización)

Es un modelo de **control de acceso completo**.

🔹 Explicación de cada parte

🔐 Autenticación

- Verifica **quién eres**
- Usuario y contraseña

🔓 Autorización

- Verifica **a qué puedes acceder**
- Permisos, roles, perfiles

📊 Auditoría / Contabilización

- Registra **qué haces**
- Logs, accesos, acciones

🔹 Relación directa con la práctica del ASA

En vuestra práctica:

- Usuario se autentica (pepito / pepita)
- El ASA autoriza:
  - Solo su web asignada
- El firewall puede registrar accesos

👉 AAA aplicado **de forma real**, no teórica.

🔹 Respuesta tipo examen

AAA es un modelo de seguridad que controla la autenticación, autorización y contabilización de los usuarios en un sistema o red.

9️⃣ ¿Qué se entiende por VPN?

🔹 Definición base

Una **VPN (Virtual Private Network)** crea un **túnel cifrado** para que los datos viajen de forma segura entre dos extremos a través de una red pública.

🔹 Qué hace realmente una VPN

- Cifra los datos
- Evita sniffing
- Protege credenciales

- Simula estar dentro de la red privada

📌 Aunque los datos viajen por Internet, **no son legibles**.

🔹 Relación con lo visto en clase (WebVPN)

En el ASA habéis usado **WebVPN**, que:

- No conecta toda la red
- Solo publica servicios concretos
- Usa HTTPS

👉 Es una VPN **de acceso controlado**, no total.

🔹 Relación con sniffing (pregunta 1)

- Sniffer ve paquetes
- VPN:
  - Los cifra
  - Los hace inútiles para el atacante

📌 VPN = antídoto directo contra sniffing.

🔹 Respuesta tipo examen

Una VPN es una tecnología que cifra los datos que viajan entre dos extremos de la red, permitiendo una comunicación segura a través de Internet.

🔟 ¿Qué es una SAI?

🔹 Definición base

Una **SAI (Sistema de Alimentación Ininterrumpida)** es un dispositivo que proporciona **energía eléctrica temporal** cuando se produce un corte o una anomalía en el suministro eléctrico.

📌 Su objetivo principal es:

> **Garantizar la disponibilidad de los sistemas**

🔹 Qué protege una SAI

Una SAI protege frente a:

- Cortes de luz
- Bajadas de tensión
- Subidas de tensión
- Microcortes eléctricos

👉 Evita:

- Apagados bruscos
- Pérdida de datos

- Daños en hardware

🔹 Relación con la ciberseguridad

Aunque no es “seguridad informática” directa, la SAI es **seguridad física**, que forma parte de la seguridad global.

📌 En ciberseguridad:

> Si el sistema no tiene energía, **no existe seguridad posible**.

🔹 Relación con lo visto en clase (Firewall / ASA)

En una empresa real:

- El firewall ASA
- Los servidores
- Los switches

👉 **Siempre** van conectados a una SAI.

Porque:

- Un firewall apagado = red expuesta
- Un apagado brusco = corrupción de configuración

🔹 Tipo de seguridad

La SAI es:

- ✔ **Seguridad pasiva**
- No bloquea ataques
- Actúa cuando hay un fallo

🔹 Respuesta tipo examen

Una SAI es un sistema de alimentación ininterrumpida que permite mantener los equipos encendidos durante un corte eléctrico, protegiendo datos y hardware.

1️⃣1️⃣ ¿Qué es SSH?

🔹 Definición base

SSH (Secure Shell) es un protocolo que permite **acceder de forma remota y segura** a un equipo o dispositivo de red.

📌 Sustituye a Telnet de forma segura.

🔹 Qué hace SSH a nivel técnico

- Cifra la comunicación

- Protege usuario y contraseña
- Evita sniffing
- Evita manipulación del tráfico

👉 Todo viaja **encriptado**.

🔹 Relación con sniffing (pregunta 1)

- Telnet → texto plano → sniffer ve todo
- SSH → cifrado → sniffer ve datos inútiles

📌 SSH es una defensa directa contra sniffing.

🔹 Relación con lo visto en clase (AAA)

SSH:

- Usa autenticación
- Puede integrarse con:
  - RADIUS
  - TACACS
- Permite control de accesos administrativos

👉 Es clave en entornos empresariales.

🔹 Por qué es “muy codiciado” por las empresas

Porque:

- Permite administración remota
- Es segura
- Es estándar
- Es auditable

📌 En redes reales:

> **Nunca se administra nada por Telnet**.

🔹 Respuesta tipo examen

SSH es un protocolo de comunicación remota segura que permite administrar equipos de forma cifrada, protegiendo credenciales y datos.

1️⃣2️⃣ ¿Qué se entiende por Telnet?

🔹 Definición base

Telnet es un protocolo de acceso remoto **no seguro**, que transmite la información **en texto plano**.

🔹 Qué problema tiene Telnet

- No cifra la comunicación
- Usuario y contraseña viajan visibles
- Es vulnerable a sniffing
- Está obsoleto

📌 Cualquier atacante puede ver las credenciales.

🔹 Relación con lo visto en clase

En una red con:

- Firewall
- VPN
- AAA

👉 Telnet **rompe toda la seguridad**, porque:

- El problema no es la red
- El problema es el protocolo

🔹 Comparación clara (SSH vs Telnet)

Característica	SSH	Telnet
Cifrado	✔ Sí	❌ No
Seguro	✔	❌
Uso actual	✔	❌
Empresas	✔	❌

🔹 Respuesta tipo examen

Telnet es un protocolo de acceso remoto que no cifra la comunicación, por lo que no es seguro y no se utiliza en entornos empresariales.

1️⃣3️⃣ ¿Qué es más seguro: que solo el usuario conozca su contraseña o que también la conozca el administrador?

🔹 Respuesta correcta

👉 **Es más seguro que solo el usuario conozca su contraseña.**

🔹 Explicación técnica

Cuando solo el usuario conoce su contraseña:

- Se respeta la privacidad
- Se reduce el riesgo interno
- Se evita abuso de privilegios
- Se cumple el principio de confianza mínima

📌 El administrador **no necesita** saber contraseñas.

🔹 Relación con AAA y seguridad moderna

En sistemas modernos:

- Las contraseñas:
  - Se almacenan cifradas
  - Se almacenan como hash
- Ni siquiera el sistema conoce la contraseña real

👉 El administrador:

- Gestiona permisos
- No gestiona secretos

🔹 Relación con el laboratorio del ASA

En vuestra práctica:

- El ASA:
  - Autentica usuarios
  - No necesita “saber” su contraseña en claro
- Aplica permisos por perfil

📌 Seguridad basada en roles, no en conocimiento de contraseñas.

🔹 Respuesta tipo examen

Es más seguro que solo el usuario conozca su contraseña, ya que reduce riesgos y protege la privacidad y la seguridad del sistema.

1️⃣4️⃣ ¿Puede un administrador visualizar la contraseña de un usuario?

🔹 Respuesta correcta

👉 **No, no puede.**

🔹 Explicación técnica

En sistemas bien diseñados:

- Las contraseñas:
  - No se guardan en texto plano
  - Se almacenan cifradas o como hash
- El administrador:
  - Puede resetear
  - No puede ver

📌 Ver contraseñas sería una mala práctica de seguridad.

🔹 Relación con lo visto en clase

Esto conecta directamente con:

- AAA
- Autenticación segura
- Buenas prácticas empresariales

👉 Si un administrador pudiera ver contraseñas:

- No habría seguridad
- No habría confianza
- No habría auditoría real

🔹 Respuesta tipo examen

No, un administrador no puede visualizar la contraseña de un usuario, solo puede modificarla o restablecerla, ya que se almacenan de forma segura.

1️⃣5️⃣ ¿Qué puertos deshabilita NetBIOS y por qué se desactiva?

🔹 ¿Qué es NetBIOS? (contexto necesario)

NetBIOS (Network Basic Input/Output System) es un sistema **antiguo** de comunicación en redes locales Windows que se utilizaba para:

- Resolución de nombres de equipos
- Compartición de archivos e impresoras
- Descubrimiento de otros equipos en la red

👉 Fue útil hace años, **cuando no existían**:

- DNS bien implementado
- Active Directory moderno
- Políticas de seguridad avanzadas

Hoy en día:

- ❌ No es necesario
- ❌ Aumenta la superficie de ataque
- ❌ Filtra información de la red interna

🔹 Puertos que utiliza NetBIOS

NetBIOS abre **tres puertos clásicos**, todos **muy conocidos por atacantes**:

Puerto	Protocolo	Función
137	UDP	NetBIOS Name Service (resolución de nombres)
138	UDP	NetBIOS Datagram Service

Puerto	Protocolo	Función
139	TCP	NetBIOS Session Service

📌 Estos puertos:

- Exponen nombres de equipos
- Exponen usuarios
- Permiten enumeración de recursos
- Se usan en ataques clásicos (reconocimiento, movimiento lateral)

👉 Por eso el profesor dice claramente que **“no sirven para nada”** hoy en día.

🔹 Relación directa con lo visto en clase (Firewall y ASA)

En las clases anteriores habéis visto un principio clave:

> **Deny by default**
> Todo lo que no es necesario, se bloquea.

NetBIOS:

- ❌ No es necesario
- ❌ No aporta seguridad
- ❌ No se usa en arquitecturas modernas

👉 Igual que:

- El ASA bloquea tráfico OUTSIDE → INSIDE
- Nosotros bloqueamos NetBIOS **en el propio host**

Esto es **seguridad en capas**:

- Firewall perimetral (ASA)
- Configuración del sistema operativo
- Reducción de superficie de ataque

🔹 ¿Por qué es peligroso dejar NetBIOS activo?

Si NetBIOS está activo, un atacante en la red puede:

- Ver nombres de equipos
- Ver usuarios conectados
- Enumerar recursos compartidos
- Preparar ataques más dirigidos

📌 En términos de ciberseguridad:

> NetBIOS **facilita la fase de reconocimiento**, que es el primer paso de cualquier ataque.

Esto conecta directamente con:

- **Sniffing**
- **Spoofing**
- **Movimiento lateral**

🔹 Cómo se deshabilita NetBIOS en Windows (paso a paso exacto)

El profesor pide hacerlo **tanto en Ethernet como en WiFi**, porque **cada adaptador tiene su propia configuración**.

🖱️ Ruta completa en Windows

1. **Centro de redes y recursos compartidos**
2. **Cambiar configuración del adaptador**
3. Click derecho en:
   - **Ethernet** → Propiedades
   - **Wi-Fi** → Propiedades
4. Seleccionar:
   - **Protocolo de Internet versión 4 (TCP/IPv4)**
5. Pulsar **Propiedades**
6. Botón **Opciones avanzadas**
7. Pestaña **WINS**
8. Marcar:
   - ✅ **Deshabilitar NetBIOS a través de TCP/IP**
9. Aceptar todo

📌 Esto debe hacerse **en cada interfaz**, no solo en una.

🔹 Qué ocurre a nivel de red al deshabilitar NetBIOS

Cuando deshabilitas NetBIOS:

- ❌ El equipo deja de:
  - Responder por los puertos 137, 138 y 139
- ❌ No anuncia su nombre en la red
- ❌ No responde a peticiones NetBIOS
- ✔ Reduce la información visible para otros equipos

👉 El PC se vuelve:

- Menos visible
- Menos identificable
- Más seguro

🔹 Relación con la filosofía del firewall ASA

Esto es exactamente lo mismo que hace el ASA en vuestra práctica:

- El ASA:
  - Bloquea ICMP
  - Bloquea accesos no permitidos
- El PC:
  - Bloquea servicios innecesarios
  - No “responde” si no hace falta

📌 Seguridad moderna:

> **No anunciar, no exponer, no responder si no es necesario**

🔹 Por qué el profesor insiste en hacerlo también en WiFi

Porque:

- WiFi suele ser:
  - Más expuesto
  - Menos controlado
  - Más fácil de atacar
- Un portátil puede:
  - Cambiar de red
  - Conectarse a redes públicas
  - Arrastrar configuraciones inseguras

👉 Si NetBIOS está activo en WiFi:

- Se expone el equipo en redes externas
- Aumenta el riesgo real

🔹 Respuesta final “de examen”

NetBIOS utiliza los puertos 137, 138 y 139.
Se deshabilita porque no es necesario en redes modernas y supone un riesgo de seguridad, ya que expone información del sistema.
Debe desactivarse tanto en la interfaz Ethernet como en WiFi desde las opciones avanzadas de TCP/IP (pestaña WINS), marcando “Deshabilitar NetBIOS a través de TCP/IP”.

1️⃣6️⃣ ¿Qué diferencia existe entre RADIUS y TACACS?

🔹 Contexto previo (muy importante)

Tanto **RADIUS** como **TACACS** son **protocolos AAA**, es decir, se utilizan para:

- **Autenticación** → verificar quién eres
- **Autorización** → verificar qué puedes hacer
- **Auditoría / Contabilización** → registrar acciones

📌 No son firewalls, no cifran tráfico general, **gestionan identidades y accesos**.

🔹 RADIUS — Características principales

🧠 ¿Para qué se usa RADIUS?

RADIUS se utiliza principalmente para:

- Acceso a redes **inalámbricas (WiFi)**
- Acceso de usuarios finales

- Control de acceso a red (NAC)
- Autenticación centralizada

📌 Ejemplo típico:

> Usuario se conecta a una WiFi corporativa → RADIUS valida usuario y contraseña.

🔐 Qué protege RADIUS

- Usuario
- Contraseña (cifrada)
- Acceso a la red

📌 No controla comandos ni acciones detalladas.

🌐 Relación con lo visto en Packet Tracer

En Packet Tracer, cuando configuras:

- AAA en un **Server-PT**
- Seleccionas **RADIUS**
- Lo asocias a accesos inalámbricos

👉 Estás simulando **un entorno WiFi corporativo real**.

📡 Puerto usado por RADIUS

- UDP **1812** (autenticación)
- UDP **1813** (contabilidad)

(En versiones antiguas: 1645 / 1646)

🧪 Ejemplo práctico (examen)

- Empresa con WiFi
- Usuarios con credenciales
- Acceso controlado

👉 **RADIUS**

🔹 TACACS — Características principales

🧠 ¿Para qué se usa TACACS?

TACACS+ se utiliza principalmente para:

- Acceso administrativo a:
  - Routers
  - Switches
  - Firewalls
- Gestión de dispositivos de red
- Control detallado de comandos

📌 Ejemplo típico:

> Administrador entra por SSH a un router → TACACS decide qué comandos puede ejecutar.

🔐 Qué controla TACACS

- Quién accede
- Qué comandos ejecuta
- Qué nivel de privilegio tiene
- Registro detallado de acciones

📌 Es **mucho más granular** que RADIUS.

🔒 Relación directa con el ASA y las clases

En un entorno real con ASA:

- Administradores NO acceden con usuarios locales
- Acceden con:
  - SSH
  - Autenticación centralizada
  - TACACS

👉 Así:

- Se controla quién toca el firewall
- Se registran cambios
- Se evita abuso

📡 Puerto usado por TACACS

- TCP **49**

📌 Usa TCP porque:

- Necesita fiabilidad
- Registra comandos uno a uno

🔹 Diferencia clave RADIUS vs TACACS (tabla clara)

Característica	RADIUS	TACACS
Tipo de acceso	Usuarios finales	Administradores
Uso típico	WiFi / acceso red	Routers, switches, ASA
Control de comandos	❌ No	✔ Sí
Granularidad	Baja	Alta
Protocolo	UDP	TCP
AAA completo	Parcial	Completo

🔹 Analogía sencilla (muy de examen)

- **RADIUS**
  👉 “¿Puedes entrar en el edificio?”
- **TACACS**
  👉 “¿Qué puertas puedes abrir y qué botones puedes tocar?”

🔹 Relación con el laboratorio visto en clase

En vuestra práctica:

- Usuarios WebVPN → autenticación básica
- En un entorno más avanzado:
  - Usuarios WiFi → RADIUS
  - Administradores ASA → TACACS

📌 Es una **evolución natural del laboratorio**.

🔹 Respuesta tipo examen (redonda)

RADIUS se utiliza principalmente para autenticar usuarios en accesos a red, como conexiones inalámbricas, mientras que TACACS se emplea para el acceso administrativo a routers y switches, permitiendo un control más detallado de permisos y comandos.

🧠 Conclusión global del repaso

Con todo lo visto:

- Firewall (ASA) → controla tráfico
- AAA → controla identidad
- RADIUS → controla acceso de usuarios
- TACACS → controla acceso de administradores
- Deshabilitar servicios (NetBIOS) → reduce superficie de ataque

👉 **La seguridad no es una herramienta, es un conjunto de decisiones bien diseñadas.**
